CLAIMS

1. A data processing apparatus for executing reproduction of a contents data from a memory device or recording of a contents data into said memory device comprising:

an enabling key block distribution key enciphering key enciphered by an enabling key blocks containing enciphered data of renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices, wherein said enabling key block also contains data of upper-rank key enciphered via lower-rank key; wherein

said data processing apparatus further comprises key distribution approval data files containing header data consisting of link count key for designating the number of contents data that should be enciphered by said enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in said enabling key blocks, thereby said key distribution approval data files are stored in said memory device.

2. The data processing apparatus according to Claim 1, wherein

said key distribution approval data files include a contents key enciphering key data obtained by enciphering contents key for enciphering processing of contents by said key enciphering key.

3. The data processing apparatus according to Claim 1, wherein

said data processing apparatus executes to update said link count data in said key distribution approval data files in correspondence with variation of the number of contents data that is enciphered by enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in the above-cited enabling key blocks.

4. The data processing apparatus according to Claim 1, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device.

5. The data processing apparatus according to Claim 1, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is identified to be inapplicable, said data processing apparatus reads said key distribution approval data files.

6. The data processing apparatus according to Claim 1, wherein

version of said enabling key block distribution key enciphering key which is enciphered and presented by said enabling key block is subject to a controlling process by way of renewing every version.

7. The data processing apparatus according to Claim 1, wherein

said data processing apparatus enciphers a plurality of leaf-keys by applying a storage key proper to said data processing apparatus and then stores said enciphered leaf-keys in a memory means inside of said data processing apparatus, wherein said leaf-keys are respectively provided in correspondence with own leaves among a hierarchy key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses.

8. The data processing apparatus according to Claim 1, wherein

a device key block is stored in a memory means of said data processing apparatus, wherein said device key block itself corresponds to an assemblage of enciphered keys comprising mutually different node keys individually enciphered in plural steps on such paths ranging from own leaves to upper-rank keys of said key tree structure based on such leaf-keys provided in correspondence with own leaves among said key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of data processing apparatuses as own leaves.

9. A data processing method for executing reproduction of a contents data from a memory device or recording of a contents data into said memory device, said method comprising:

a step for enciphering an enabling key block distribution key enciphering key by an enabling key blocks containing enciphered data of renewal keys on such paths for constituting a key tree structure comprising a variety of keys disposed in correspondence with roots, nodes, and leaves on such paths ranging from roots to leaves of said key tree structure comprising a plurality of devices, wherein said enabling key block also contains data of upper-rank key enciphered via lower-rank key; and

a step for storing the key distribution approval data files containing header data consisting of link count key for designating the number of contents data that is enciphered by said enciphering keys in said memory device based on said enabling key block distribution key enciphering key.

10. The data processing method according to Claim 9, wherein

said key distribution approval data files include a contents key enciphering key data obtained by enciphering contents key for enciphering processing of contents by said key enciphering key.

11. The data processing method according to Claim 9, wherein

said data processing apparatus executes to update said link count data in said key distribution approval data files in correspondence with variation of the number of contents data that is enciphered by enciphering keys acquirable based on said enabling key block distribution key enciphering key stored in the above-cited enabling key blocks.

12. The data processing method according to Claim 9, wherein

said data processing apparatus stores said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device.

13. The data processing method according to Claim 9, wherein

said key enciphering key is stored in said memory, wherein said key enciphering key is acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

whenever processing contents data stored in said memory device, said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device, wherein, solely in the case in which said key enciphering key is identified to be inapplicable, said data processing apparatus reads said key distribution approval data files.

14. A program providing medium which provides such a computer program to enable a computer system to execute a data processing process via reproduction of a contents data from a memory device or via recording of a contents data into a memory device, said process comprising:

a step for storing said key enciphering key in said memory, wherein said key enciphering key are acquired by way of decode processing said enabling key block distribution key enciphering key contained in a key distribution approval data file containing a greater count number shown by a link-count data present among said key distribution approval data files stored in said memory device; and

a step for executing reading said key distribution approval data files solely in the case where said key enciphering key is identified to be inapplicable, wherein said data processing apparatus judges applicability of said key enciphering key previously stored in said memory device, and then, if it is identified to be applicable, said data processing apparatus utilizes said key enciphering key previously stored in said memory device.